

Corporate intranet platform – open and commercial solutions comparison

Korporacyjna platforma intranetowa - porównanie rozwiązania otwartego i komercyjnego

Konrad Czarny*

Department of Computer Science, Lublin University of Technology, Nadbystrzycka 36B, 20-618 Lublin, Poland

Abstract

The article presents a comparison of CMS systems that can be used when creating an intranet platform for a corporate network. The primary goal is to indicate which of the technologies is the most suitable for a large international corporation. Two open (WordPress, Drupal) and commercial (SharePoint, Confluence) tools were included in the study.

Keywords: SharePoint; Drupal; Confluence; WordPress

Streszczenie

Artykuł przedstawia porównanie gotowych rozwiązań możliwych do wykorzystania podczas tworzenia platformy intranetowej stosowanej przez sieć korporacyjną. Kluczowym celem jest wskazanie, która z przedstawionych technologii jest najbardziej odpowiednia dla dużej, międzynarodowej korporacji. W badaniach uwzględniono po dwa otwarte (WordPress, Drupal) oraz komercyjne (SharePoint, Confluence) narzędzia.

Słowa kluczowe: SharePoint; Drupal; Confluence; WordPress

*Corresponding author

Email address: czarny.konrad95@gmail.com (K. Czarny)

©Published under Creative Common License (CC BY-SA v4.0)

1. Wstęp

Artykuł porównuje rozwiązania otwarte oraz korporacyjne możliwe do wykorzystania przy tworzeniu korporacyjnej sieci intranetowej. Technologie do porównania wybrane zostały na podstawie analiz ich popularności przedstawianych corocznie przez stronę w3techs.com [1, 2] z uwzględnieniem ich wykorzystania do tworzenia sieci intranetowej. W przypadku rozwiązań otwartych wybrano narzędzie WordPress i Drupal, natomiast w przypadku rozwiązań komercyjnych SharePoint oraz Confluence [1, 2, 3, 4].

2. Cel badań oraz metody i narzędzia badawcze

Celem badań było porównanie wskazanych systemów CMS (ang. Content Management System), pozwalających na implementację sieci intranetowej oraz wybranie najbardziej odpowiedniego dla wymagań charakteryzujących międzynarodową korporację.

Do przeprowadzenia analizy porównawczej wybrano metodę analizy wielokryterialnej. W tym celu przeanalizowano wymagania, jakie musi spełniać aplikacja intranetowa. Analiza ta została przeprowadzona na przykładzie innych publikacji naukowych [3], oraz z wykorzystaniem przykładowej aplikacji, funkcjonującej w międzynarodowej korporacji.

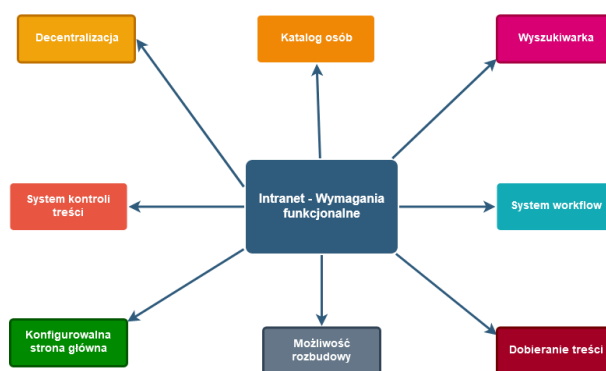
W celu wykonania analizy funkcjonalności wybranych technologii, wykorzystano publicznie dostępne informacje, takie jak dokumentacje [5-8] i artykuły [9]. Zebrane dane oceniono pod kątem spełnienia wymagań stawianych aplikacjom intranetowym.

3. Aplikacja intranetowa

Pierwszym krokiem potrzebnym do przeprowadzenia analizy porównawczej wybranych technologii jest określenie wymagań funkcjonalnych i нефункциональных, wymogów bezpieczeństwa oraz procesów korporacyjnych, które mają bezpośrednie przełożenie na sposób realizacji określonych wymagań [3].

3.1. Specyfikacja wymagań funkcjonalnych

Korporacyjna platforma intranetowa wymaga sprawnego podejścia do aktualizowania i uruchamiania nowych funkcji, które będą służyć jej użytkownikom. Istotne jest także zachowanie pewnej równowagi pomiędzy funkcjonalnością aplikacji, a jej bezpieczeństwem i wydajnością. Szczegółowe wymagania funkcjonalne charakteryzujące aplikację intranetową skierowaną do międzynarodowej korporacji przedstawia rysunek 1.

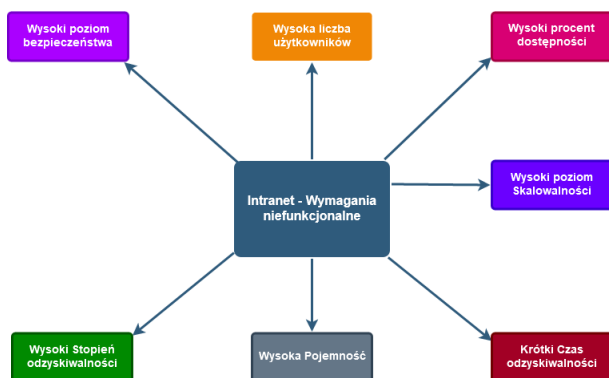


Rysunek 1: Schemat wymagań funkcjonalnych aplikacji intranetowej

Wymaganie te, zostały wykorzystane jako kryteria służące analizie porównawczej, oraz szerzej opisane w rozdziale 5.

3.2. Specyfika wymagań niefunkcjonalnych

Mimo iż wymagania niefunkcjonalne nie posiadają bezpośredniego wpływu na funkcjonalność systemu, to nakładają na niego szereg zaleceń, opisujących w jaki sposób owe wymagania mają być realizowane. Wynika to bezpośrednio z wymagań oraz procesów obowiązujących w danej organizacji, oraz z ograniczeń występujących w zastosowanej technologii. Szczegółowe wymagania niefunkcjonalne charakteryzujące aplikację intranetową dla międzynarodowej korporacji zostały przedstawione na rysunku 2.

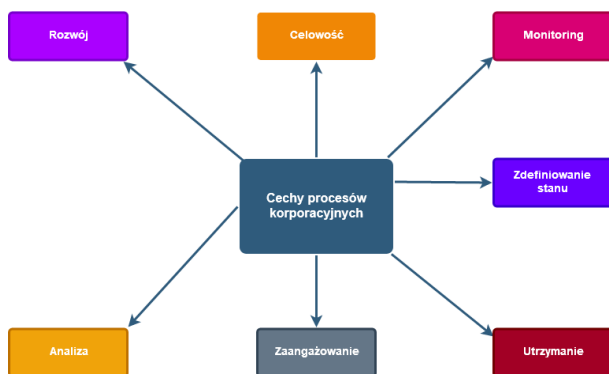


Rysunek 2: Schemat wymagań niefunkcjonalnych aplikacji intranetowej

Wymaganie te, zostały wykorzystane jako kryteria służące analizie porównawczej, oraz szerzej opisane w rozdziale 5.

3.3. Charakterystyka procesów korporacyjnych

Proces biznesowy lub korporacyjny odnosi się do szerokiego zakresu ustrukturyzowanych, często powiązanych ze sobą działań lub zadań wykonywanych przez ludzi bądź sprzęt, w celu wytworzenia usługi czy produktu dla konkretnego konsumenta. Procesy biznesowe są wdrażane w celu osiągnięcia założonego celu organizacyjnego. Zachodzą one na wszystkich poziomach organizacyjnych. Niektóre z nich są widoczne dla klientów, inne natomiast nie.



Rysunek 3: Schemat procesów korporacyjnych aplikacji intranetowej

Międzynarodowa organizacja posiada wiele procesów ukierunkowanych na osiągnięcie różnych celów. Na rysunku 3 zostały przedstawione ich charakterystyki, które mają wpływ na projekt aplikacji [4].

3.4. Wymagania dotyczące bezpieczeństwa

System taki jak Intranet zawiera zazwyczaj poufne informacje o znaczeniu krytycznym dla firmy, takie jak: szczegółowe informacje o realizowanych projektach, dane osobowe pracowników, wiedzę instytucjonalną, prywatne rozmowy czy dokumenty zawierające własność intelektualną i inne informacje zastrzeżone. Jest to system, który wymaga solidnych zabezpieczeń. Istnieje wiele wszelkiego rodzaju zagrożeń wewnętrznych i zewnętrznych – wewnętrzne naruszenia bezpieczeństwa, nieautoryzowany dostęp, czy słabe hasła mogące zagrozić systemowi. Zarządzanie i ochrona danych internetowych są niezbędne dla każdej firmy. Każda firma jest zagrożona nie tylko złośliwymi atakami z zewnątrz, ale także wewnętrznymi naruszeniami ze strony pracowników (zamierzonymi lub nie). Każde oprogramowanie intranetowe musi mieć zintegrowane rozwiązanie bezpieczeństwa, aby zapewnić maksymalną możliwą ochronę. Może to wydawać się oczywiste, jednak protokoły logowania są pierwszą linią obrony intranetu. Funkcjonalność ta jest pierwszą barierą broniącą portal przed zagrożeniami. Rozwiązanie takie powinno wspierać integrację z „pojedynczym logowaniem” (ang. *single sign-on*, SSO), Active Directory (AD) lub Lightweight Directory Access Protocol (LDAP) w celu zapewnienia płynnego i centralnie zarządzanego procesu uwierzytelnienia. System ten powinien również zapewniać solidną kontrolę nad dostępem wewnętrznym oraz dostępem partnerów zewnętrznych. Pracownicy i partnerzy powinni móc uzyskać dostęp do intranetu za pośrednictwem platform mobilnych lub stacjonarnych **bezpiecznie**, bez względu na to gdzie się znajdują. Aplikacja, powinno spełniać takie wymogi bezpieczeństwa jak [10]:

- EU-USA & SWISS-US Privacy Shield;
- certyfikaty GLBA (ang. Gramm-Leach-Bliley Act);
- certyfikaty HIPAA (ang. Health Insurance Portability and Accountability Act);
- zgodność z RODO (ang. General Data Protection Regulation, GDPR).

W celu zapewnienia odpowiedniego poziomu bezpieczeństwa, organizacja korzystająca z intranetu będzie chciała wykorzystać wiele warstw obrony w celu ochrony kluczowych informacji i obsługi wszystkich krytycznych aspektów bezpieczeństwa sieci i aplikacji, w tym uwierzytelniania i autoryzacji. Mocny poziom bezpieczeństwa intranetu powinien obejmować takie kwestie jak przestrzeganie normy ISO 27001, regularne audyty stron trzecich oraz spójne aktualizacje w oparciu o trendy w branży. Zapewnia to, iż program bezpieczeństwa systemu dotrzyma kroku aktualnym standardom zabezpieczeń. Dobrą praktyką jest również zaimplementowanie systemu zarządzania bezpieczeństwem informacji (SZBI) [13]. Opisuje on ramy zasad i procedur,

które obejmują wszystkie prawne i fizyczne oraz techniczne kontrole zaangażowane w procesy zarządzania ryzykiem informacyjnym w organizacji, a także systematycznie ocenia i ustala priorytety zagrożeń bezpieczeństwa informacji, biorąc pod uwagę indywidualne podatności danej firmy. Należy również upewnić się, iż o bezpieczeństwo intranetu dbają certyfikowani specjaliści, którzy posiadają wiedzę specjalistyczną w zakresie bezpieczeństwa aplikacji, sieci oraz architektury. Specjaliści Ci mogą zdefiniować wiodące w branży zasady bezpieczeństwa i jego kontrole, co jest kluczowym zagadnieniem pozwalającym zabezpieczeniu danego systemu na obronę przed nowymi zagrożeniami.

4. Przegląd analizowanych technologii

W artykule przeanalizowano możliwości oferowane przez dwa systemy otwarto źródłowe (WordPress i Drupal) oraz dwa systemy komercyjne (SharePoint i Confluence).

4.1. WordPress

WordPress, jest to najpopularniejsze na świecie narzędzie do tworzenia stron internetowych, oparte na języku PHP oraz relacyjnej bazie danych MySQL na licencji GNU (General Public License) [9]. Zawiera wbudowaną architekturę rozszerzeń oraz motywów. Używany jest on przez ponad 60 milionów witryn internetowych, co stanowi 33.6% z 10 milionów najpopularniejszych stron sieciowych [3]. Za jego pomocą można przygotować prosty blog, sklep internetowy (z popularną wtyczką WooCommerce), a także w pełni funkcjonalną stronę biznesową. Opanowanie podstaw jego użytkowania nie wymaga prawie żadnych umiejętności programistycznych, czy projektowych. Dzięki możliwości wyboru tysięcy darmowych projektów witryn, zwanych motywami, oraz wtyczek zapewniających szeroką gamę funkcjonalności, do stworzenia własnej witryny sieciowej wystarczy podstawowa wiedza informatyczna. Dzięki stworzeniu natywnych aplikacji pod systemy takie jak Android czy iOS, zaprojektowanych przez firmę Automattic, możliwy jest wygodny i bezproblemowy dostęp do tworzonych witryn również za pośrednictwem platform mobilnych.

4.2. Drupal

Drupal to kolejny otwarto źródłowy system zarządzania treścią, oparty na języku PHP oraz licencji GNU General Public License [10]. Dostarcza on kod po stronie serwera dla minimum 2.3% wszystkich stron internetowych na świecie, takich jak blogi, strony korporacyjne, witryny partii politycznych czy rządowych [4]. Obecnie drupal posiada 114 tysięcy aktywnie rozwijających go użytkowników, co skutkuje stworzeniem ponad 42 tysięcy darmowych modułów rozszerzających jego wbudowane funkcjonalności, czy prawie 3 tysięcy darmowych układów stron [10]. Jego podstawowe wydanie, znane jako Drupal Core, zawiera szereg znanych z innych systemów CMS funkcjonalności, takich jak system kont, zarządzanie menu, kanały RSS, taksono-

nię, modyfikację układu strony czy system administracji.

4.3. SharePoint

SharePoint to wprowadzona na rynek w 2001 roku, multiplatformowa, internetowa, komercyjna platforma kolaboracyjna, integrująca się z pakietem Microsoft Office [7]. Sprzedawana jest ona przede wszystkim jako system zarządzania treścią i przechowywania dokumentów. Produkt ten jest wysoce konfigurowalny, a jego użycie może różnić się znacznie w zależności od używającej go organizacji. Według statystyk podawanych przez tworzącą go firmę – Microsoft, SharePoint ma 190 milionów użytkowników wśród 200 tysięcy organizacji klienckich [1].

SharePoint można podzielić na dwie główne edycje:

- SharePoint Serwer - udostępniany organizacjom wymagającym większej kontroli nad funkcjonalnościami i wyglądem aplikacji. Produkt ten instalowany jest w infrastrukturze klienckiej. Jest rzadziej aktualizowany niż jego bratnia wersja, posiada jednak dostęp do szeregu unikalnych dla siebie funkcji i możliwości dostosowywania;
- SharePoint Online – hostowana przez Microsoft, wersja systemu SharePoint, zawarta zazwyczaj w planie subskrypcji Microsoft Office 365, posiada jednak również możliwość kupna bezpośredniego. Zaletą tej wersji usługi jest to, iż nie wymaga ona utrzymywania własnej infrastruktury serwerowej. Rezultatem tego jednak jest mniej opcji dostosowania produktu. Ograniczony jest do podstawowego zestawu scenariuszy współpracy, hostingu plików oraz zarządzania dokumentami i treścią.

4.4. Confluence

Confluence to komercyjne oprogramowanie do współpracy między użytkownikami stworzone przez australijską firmę Atlassian w języku Java [8]. Pierwsza wersja została opublikowana w 2004 roku. Podstawowa wersja, Confluence Standalone, jest wyposażona we wbudowany serwer internetowy Tomcat, oraz bazę danych HSQL, obsługuje jednak również inne bazy danych. Confluence jest sprzedawany jako oprogramowanie dla przedsiębiorstw, oraz licencjonowany jako oprogramowanie lokalne lub usługa oferowana w chmurze.

5. Kryteria porównawcze

Z punktu widzenia wymagań związanych z użytkowaniem aplikacji intranetowej, system powinien udostępniać:

- **Katalog osób** – rozbudowany katalog osób, z opcją pobierania danych z wielu źródeł, oraz możliwość dodawania informacji, takich jak języki czy kwalifikacje, jest niezbędna w systemie;
- System Workflow – umożliwia organizacjom usprawnienie kluczowych procesów biznesowych. Pozwala to użytkownikom, którzy nie posiadają umiejętności technicznych, na proste i intuicyjne

tworzenie formularzy automatyzujących procesy biznesowe. Dzięki temu firma jest w stanie zachować wysoką wydajność, eliminując jednocześnie potrzebę zatrudniania osób z branży IT, lub administratorów systemu. Istnienie Workflow jest bardzo pożądane;

- System kontroli treści – Intranet musi zawierać także prosty w obsłudze oraz zorientowany na użytkownika system zarządzania treścią, z takimi funkcjonalnościami jak tagowanie, słowa kluczowe czy ocenianie stron w celu możliwości wyszukania ich pod kątem najlepszych ocen dla określonych haseł. Dostępne powinny być również dodatkowe funkcjonalności, takie jak daty interakcji czy kontrola wersji, które pomagają zachować aktualność całej zawartości witryny.
- Dobieranie treści – wraz z rozrostem organizacji, zwiększa się także liczba projektów, stanowisk czy grup pracowników. Kierowanie wszystkich informacji do każdego pracownika, niezależnie od biura w którym się znajduje czy używanego przez niego języka jest wysoce nieefektywne. Treści powinny być ukierunkowywane na unikalne potrzeby określonego pracownika.
- Wyszukiwarkę – wydajna i wszechstronna wyszukiwarka, powinna umożliwić dostęp do wyselekcjonowanych treści intranetu, oraz systemów pamięci masowej w chmurze.
- Konfigurowalną stronę główną – dzięki odpowiednim informacjom, widżetom i treściom dobranym specjalnie dla określonych grup, strona główna powinna zapewniać spersonalizowaną obsługę wielu modułów. Dzięki takiej funkcjonalności nowi użytkownicy intranetu, mogą szybko otrzymywać istotne dla nich informacje. To z kolei zapewni im łatwe wdrożenie się w specyfikę pracy w danej organizacji.
- Witryny zespołu (decentralizacja) – jedną z kluczowych funkcjonalności w nowoczesnych intranetach są „witryny zespołu” (ang. teams). Pozwalają one na unikalne dla danej organizacji projektowanie struktury oraz hierarchii witryny, czyniąc ją bardziej modularną. Idea witryn zespołu polega na możliwości tworzenia wielu podstron w obrębie intranetu w celu pracy nad poszczególnymi projektami w firmie. Każda z takich witryn posiada odrębny od reszty intranetu system uprawnień oraz strukturę, a także może być modyfikowalna wedle uznania w celu spełnienia wymagań danego projektu. Zmiany takie nie wpływają na resztę intranetu czy inne witryny.
- Możliwość rozbudowy – wraz z rozwojem firmy, intranet musi podlegać ciągłemu procesowi rozbudowy w celu dostosowania do zmieniających się potrzeb korporacji. Wymaga to wysokiej modułowości systemu oraz architektury łatwej do rozbudowy i długiego okresu wsparcia. Możliwość ta powinna być oficjalnie zapewniana przez producenta.
- Możliwość korzystania dla dużej liczby użytkowników – organizacja korzystająca z intranetu, składa się zazwyczaj z wielu pracowników i kontraktorów z różnych kontynentów. Wymaga to więc, aby każdy z nich posiadał własne konto z przydzielonymi do niego informacjami i uprawnieniami. System taki musi być w stanie potencjalnie obsłużyć nawet setkę tysięcy użytkowników z różnych krajów oraz stref czasowych, co jest często nieosiągalne dla zwykłej witryny internetowej. System powinien być w stanie obsługiwać ponad 100 000 użytkowników.
- Dużą pojemność – biorąc pod uwagę wspomnianą wyżej liczbę użytkowników oraz funkcjonalności takie jak zarządzanie dokumentami i tworzenie witryn zespołu, system dodatkowo musi być w stanie przyjąć ogromną ilość danych oraz plików, rzędu dziesiątków terabajtów. Wymaga to nie tylko odpowiedniej infrastruktury sieciowej i fizycznej, ale także systemu zdolnego do symultanicznej analizy wielu informacji. System powinien być w stanie obsługiwać przynajmniej 1 terabajt danych.
- Skalowalność – wraz z rozwojem organizacji, oraz wzrostem liczby jej pracowników (a co za tym idzie, osób korzystających z intranetu), w parze z możliwością rozbudowy o nowe funkcjonalności, musi iść także skalowalność systemu pod względem liczby jego użytkowników oraz bazodanowych informacji trzymany na serwerach. Producent powinien podać jaki jest wpływ rozbudowy systemu na jego wydajność.
- Wysoki poziom bezpieczeństwa – aby chronić poufne informacje organizacji zarówno przed osobami z poza niej, jak i przed pracownikami, którzy nie powinni mieć do nich dostępu, aplikacja potrzebuje rozbudowanego systemu ról. Dzięki temu, można zagwarantować, że dostęp do danych wrażliwych mają tylko uprawnione osoby. Kryterium do wskazania poziomu bezpieczeństwa systemu jest indywidualna ocena pod kątem opisanych w podrozdziale 3.4 cech, oraz danych historycznych na temat wykrytych błędów.
- Wysoki procent dostępności – dostępność określa liczbę punktów procentowych czasu, w którym aplikacja jest dostępna dla użytkowników. Aplikacja, która ma służyć jako główny system korporacji, wymaga osiągnięcia dostępności na poziomie minimum **98%** [5]. Oznacza to iż wszelkie przestoje związane z wdrożeniami nowej wersji aplikacji, naprawą błędów czy jej konfiguracją nie powinny przekraczać 2% ogólnego czasu dostępu.
- **Wysoki stopień odzyskiwalności** – termin ten określa liczbę punktów procentowych w jakich aplikacja ma zostać przywrócona do swojego poprzedniego stanu po ewentualnym błędzie krytycznym. Dla międzynarodowej firmy operującej na dziesiątkach terabajtów danych i informacji, stopień odtworzenia gwarantowany przez aplikację musi wynosić **minimum 95%** [5]. Oznacza to, iż praktycznie wszystkie dane powinny zostać przywrócone do stanu sprzed wystąpienia błędu.
- **Krótki czas odtworzenia** – to czas, w trakcie którego aplikacja powinna zostać przywrócona do stanu poprzedniego po ewentualnym błędzie krytycznym.

Dla dużej organizacji, do której dostęp dziennie mają uzyskiwać setki tysięcy osób, czas ten nie powinien przekraczać **16 godzin** [5]. Biorąc pod uwagę 8 godzinny dzień pracy obowiązujący w większości firm, czas taki gwarantuje przywrócenie aplikacji do stanu sprzed wystąpienia błędu z dnia na dzień, między okresami największej używalności. Przeszłość powinien być możliwie minimalną niedogodnością dla użytkownika końcowego.

6. Analiza porównawcza

W celu porównania omawianych technologii, wybrano 15 opisanych w poprzednim rozdziale kryteriów, które powinny spełniać szkielet aplikacyjny stosowany do tworzenia intranetu dla międzynarodowej korporacji. Kryteria te zostały wyselekcjonowane, w oparciu o opisane wymagania funkcjonalne i нефункционаłne, charakterystykę procesów korporacyjnych oraz wymagania dotyczące bezpieczeństwa. Najwygodniejszym i najbardziej czytelnym sposobem zestawienia omawianych wymagań, jest prezentacja tabelaryczna (Tabela 1).

Tabela 1: Spełnianie wymagań przez określone technologie

	WordPress	Drupal	SharePoint	Confluence
Katalog osób	Jako plugin	Brak	Wbudowany	Brak
System workflow	Jako plugin	Wbudowany	Wbudowany	Wbudowany
System kontroli treści	Wbudowany	Niedoskonały	Wbudowany	Wbudowany
Dobieranie treści	Brak	Brak	Wbudowane	Brak
Wyszukiwarka	Wbudowana	Wbudowana	Wbudowana	Wbudowana
Konfigurowalna strona główna	Wbudowana	Wbudowana	Wbudowana	Wbudowana
Decentralizacja	Jako plugin	Wbudowana	Wbudowana	Wbudowana
Możliwość rozbudowy	Wbudowana	Wbudowana	Wbudowana	Możliwa, ale nie wspierana
>100 000 użytkowników	Tak	Tak	Tak	Zależy od licencji
Pojemność >1 TB	Tak	Tak	Tak	Tak
Skalowalność	Tak	Tak	Tak	Zależy od licencji
Poziom bezpieczeństwa	Niski	Niski	Wysoki	Wysoki
Procent dostępności	Zależy od implementacji	Zależy od implementacji	Mín 95%	Mín 95%
Stopień odzyskiwalności	Zależy od implementacji	Zależy od implementacji	Mín 98%	Mín 98%
Czas odzyskiwalności	Zależy od implementacji	Zależy od implementacji	<16 godzin	<16 godzin
Suma punktów	20	20	30	23

Każde z prezentowanych kryteriów oceniono w skali punktowej 0-2 z tą samą wagą, gdzie:

- 2 punkty oznaczają bezwarunkowe spełnienie wymagań (kolor zielony);
- 1 punkt oznacza, że dane kryterium dostępne jest np. w postaci dodatkowej wtyczki (kolor żółty);
- 0 punktów oznacza brak danej funkcji (kolor czerwony).

Dana technologia mogła uzyskać maksymalnie 30 punktów. Końcowe wyniki zestawione są w ostatnim wierszu tabeli 1.

Na ostateczne wyniki porównania duży wpływ ma fakt, że procent dostępności, stopień i czas odzyskiwania danych dla SharePoint i Confluence, są gwarantowane przez producentów. W przypadku ich odpowied-

ników o otwartym dostępie, wartości te są zależne od konkretnej implementacji oraz umiejętności osób odpowiedzialnych za obsługę systemu.

7. Wnioski

Analizując wymagania funkcjonalne, нефункционаłne oraz procesy wykorzystywane w międzynarodowych organizacjach, należy uznać, iż aplikacje o zamkniętej strukturze kodu są odpowiedniejsze do stworzenia korporacyjnego systemu intranetowego. Wysoki w porównaniu do otwartoźródłowych systemów, poziom bezpieczeństwa zapewniany przez nie jest jednym z najważniejszych warunków, jakie powinna spełniać korporacyjna platforma intranetowa. Trzymanie w tajemnicy ewentualnych luk w strukturach systemu bezpieczeństwa, wsparcie twórców tych szkieletów aplikacyjnych oraz szereg najwyższej klasy ekspertów stojących za zaimplementowanymi w nich zabezpieczeniami daje możliwie wysoką gwarancję bezpieczeństwa wrażliwych danych.

Porównując dwa wybrane z tej kategorii szkielety aplikacyjne (SharePoint oraz Confluence), lepszy jest ten pierwszy. Jego podstawowa implementacja nie tylko spełnia wymienione wymagania funkcjonalne, oraz pozytywnie odwzorowuje ich implementację poprzez wymagania нефункционаłne, ale także oferuje wystarczająco elastyczny system rozbudowy. Dzięki temu, zespół programistyczny o odpowiednich umiejętnościach będzie w stanie wypracować wszelkie nieobecne w nim funkcjonalności a następnie zaimplementować je do już istniejącego systemu.

Przeprowadzona analiza skupiała się na wybraniu odpowiedniego szkieletu aplikacyjnego do określonego typu aplikacji, wymagającej dostępu dla minimum 100 000 użytkowników i przetwarzającej setki gigabajtów danych oraz wymagającej możliwości ciągłej rozbudowy, dostosowywania, ciągłego dostępu oraz jak największego poziomu bezpieczeństwa.

W przypadku intranetowej aplikacji dla klienta korporacyjnego, najodpowiedniejszą jest platforma SharePoint, która mimo swoich kosztów eksploatacji, związanej z zespołem programistycznym i licencjami, daje największe możliwości oraz spełnia najwięcej z ocenianych w niniejszym artykule wymagań.

W przypadku technologii o otwartym dostępie, oba porównywane rozwiązania są na podobnym poziomie.

Literatura

- [1] W3techs, <https://w3techs.com/technologies/details/cm-sharepoint/all/all> [01.09.2018]
- [2] W3techs, <https://w3techs.com/technologies/details/cm-confluence/all/all> [01.09.2018]
- [3] W3techs, <https://w3techs.com/technologies/details/cm-wordpress/> [01.09.2018]
- [4] W3techs, <https://w3techs.com/technologies/details/cm-drupal/> [01.09.2018]
- [5] J. Robertson, Designing Intranets: Creating Sites that Work. Step Two Designs, 2010

- [6] A. Rockley, P. Kostur, S. Mannig, Managing Enterprise Content: A Unified Content Strategy. New Riders, 2003.
- [7] Microsoft, <https://docs.microsoft.com/en-us/sharepoint/> [01.09.2018]
- [8] Atlassian, <https://confluence.atlassian.com/> [01.09.2018]
- [9] WordPress, <https://codex.wordpress.org/> [01.09.2018]
- [10] Drupal, <https://www.drupal.org/documentation/> [01.09.2018]
- [11] C-sharpcorner, <https://www.c-sharpcorner.com/UploadFile/40e97e/sharepoint-non-functional-requirements/> [01.09.2018]
- [12] Bezpieczna chmura, <https://zaufanatrzeciastrona.pl/post/jak-bezpiecznie-przeniec-sie-do-chmury-wymagania-prawne/> [01.09.2018]
- [13] OpenSecurity, <https://opensecurity.pl/bezpieczenstwo-informacji-wg-iso-27001/> [01.09.2018]